## REMARKS

Applicants respectfully traverse the rejection of the pending claims over Bell reference (USP 6,832,319). In particular, it is respectfully pointed out that the Bell reference in no way teaches the generation of a pseudo-random number in the storage engine as recited in claim 1. To clarify this issue, the Bell disk encryption scheme will be reviewed again: Consider Bell's Figure 4, which illustrates the disk manufacture process. Each disk gets a unique media ID as shown for step 40. In addition, as also explained in Col. 6, lines 50-51, all the blank disks get the same media key block (step 42 of Figure 4). This media key block is not generated by the player.

The generation of the media key (which will be the same for all players) is described, for example, starting at Col. 8, line 26. Each player receives at manufacture, a set of device keys. Yes, Bell says each key is a "random number of predetermined bit size," but note carefully that the player does not generate these keys. They are fixed at manufacture and will not change, the player is set with them for the life of the device. The generation of the media key block (upon disk manufacture) is further described with regard to Figure 8 (steps 70, 72, and 74). The manufacturer generates "N" media numbers in step 70. Then each media number is encrypted with all device keys in step 72 (which firmly establishes this is occurring during disk manufacture, no player has access to all device keys). In step 74, the media block is written to the Bell disk.

The process of reading an encrypted Bell disk is shown in Figure 6: a player reads the media key block and the media ID, determines the media key from the media key block, combines them to get the content key, and decrypts the encrypted data using the content key.

But note the flaw in the Bell system: anyone with access to a disk reader may obtain the media key block and the media ID. Having read the media key, a hacker may then freely experiment using various hacking algorithms to get the media key. The hacker may then proceed to combine the hacked media key with the media ID to get the content key.

In sharp contrast, claim 1 recites the acts of "generating a pseudo-random number within the data storage engine" and "generating an internal key within the data storage engine using the pseudo-random number." The Bell reference is entirely silent regarding such an inventive act: the Bell player in no way generates any random numbers whatsoever. Unlike Bell, when Applicants' storage engine generates its internal key, this generation has nothing to do with reading data from the disk. A hacker may read the disk's contents exhaustively but never will have access to the internal key generation. As set forth on page 10, lines 1 through 12, even if a hacker reverse engineers the ASIC that performs the pseudo-random number generation, the seed to the number generator may be stored externally to the ASIC, thereby defeating even this advanced hacking act. In this fashion, the digital rights management is "storage-engine-based" as compared to the host-based scheme in the Bell reference in which a manufacturer (rather than the storage engine) provides the media key block. Accordingly, claim 1 is patentable over the Bell reference.

The Silverbrook reference (USP 6,334,190) does nothing to cure the deficiencies of the Bell reference. Thus, because claims 2 and 6 – 13 depend either directly or indirectly upon claim 1, these claims are patentable over the cited prior art for at least the same reasons.

Claim 1 has been amended to address a minor informality. No new matter is added.

Claim 14 and its dependent claims 15 – 19 are patentable over the cited prior art analogously as discussed with regard to claim 1. For example, claim 14 recites the act of "generating a plurality of internal keys using the pseudo-random number generator." For analogous reasons, claim 20 and its dependent claim 21 are patentable over the cited prior art.

## CONCLUSION

For the above reasons, pending Claims 1 – 2, and 6 – 21 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

I hereby certify that this correspondence is facsimile transmitted to the Commissioner for Patents, Washington, D.C. 20231, at 571-273-8300, on February 24, 2006.

Jon Hallman

Jonathan W. Hallman

February 24, 2006
Date of Signature

Respectfully submitted,

Jon Hallman

Jonathan W. Hallman
Attorney for Applicant(s)
Reg. No. 42,622